EXHIBIT 7

Understand mutual TLS at Google Cloud

Mutual TLS (mTLS) is an industry standard protocol for mutual authentication between a client and a server. The mTLS protocol ensures that both the client and server, at each end of a network connection, are who they claim they are by verifying that both possess the private key associated with the client certificate.

What is a client certificate?

A client certificate, also called a Transport Layer Security (TLS) certificate, is a file that contains important information for verifying a device's identity. The certificate information includes the public key, a statement of who issued the certificate (certificates can be issued by certificate authorities or self- signed), and the certificate's expiration date.

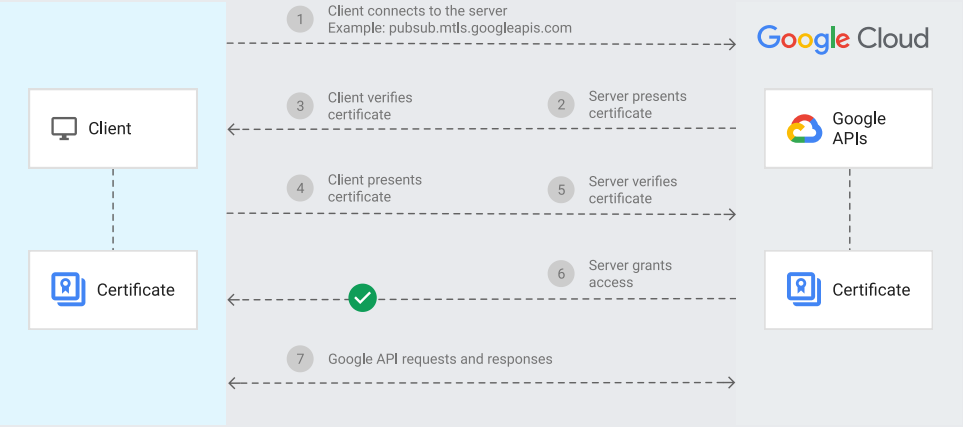
How the Google APIs validate device identity

The TLS protocol uses a technique called public key infrastructure (PKI), which relies on a pair of asymmetric keys: a public key and a private key. Anything encrypted with the private key can be decrypted only with the public key. The Google Cloud APIs use the TLS protocol to verify the identity of a device by decrypting the message encrypted by the private key using the public key of the certificate during the mTLS handshake. The successful decryption proves the possession of the private key which is only available from trusted devices.

To enable the mTLS handshake and validation process, a client must do the following:

- Establish an mTLS connection with the Google APIs by using mTLS-specific API endpoints. The mTLS-specific endpoints have the following format: `[service].mtls.googleapis.com`
- Discover and use the device certificate during the mTLS handshake. If you are using Endpoint Verification for certificate deployment, this type of certificate is automatically discovered and used by the supported clients.

The following diagram illustrates the mTLS handshake between a client and a Google API server:



What's next

- Set up certificate-based access (/beyondcorp-enterprise/docs/set-up-cba)

Last updated 2025-01-08 UTC.

Ex. 7